CLAIMS

We claim:

1. A method of controlling access to a desired resource hosted on a destination server, comprising the steps of:

(a) receiving handshaking packets from a client machine intended to begin a session with the destination server;

(b) redirecting network communications, including the steps of:

redirecting the handshaking packets by rewriting the destination address in the handshaking packets' IP headers to route the packets to an access controlling web server;

receiving a content request packet from the client machine destined for the destination server intended to retrieve the desired resource from the destination server; and

redirecting the content request packet by rewriting the destination address in the packet IP header to route the packet to the access controlling web server;

(c) receiving a response from the access controlling web server; and

(d) controlling access of the client machine to the desired resource based on the response from the access controlling web server.

2. The method according to claim 1, wherein the step of controlling access to the desired resource based on the response from the access controlling web server further comprises the step of:

establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.

3. The method according to claim 2, wherein the content request packet comprises a GET URL packet.

4. The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server does not recognize the URL of the GET URL packet.

5. The method according to claim 4, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response is that the access controlling web server recognizes the URL of the GET URL packet.

6. The method according to claim 5, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

7. The method according to claim 6, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

8. The method according to claim 6, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

9. The method according to claim 8, wherein the step of determining whether to redirect network communications comprises deciding to redirect network

communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

10. The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server recognizes the URL of the GET URL packet.

11. The method according to claim 10, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response indicates that the access controlling web server does not recognize the URL of the GET URL packet.

12. The method according to claim 11, wherein the access controlling web server is an RSACi Web Server.

13. The method according to claim 11, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

14. The method according to claim 13, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

15. The method according to claim 13, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

16. The method according to claim 15, wherein the step of determining whether to redirect network communications comprises deciding to redirect network

communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

17. A computer-readable medium having computer-executable instructions for controlling access to a desired resource hosted on a destination server comprising the steps of:

(a) receiving handshaking packets from a client machine intended to begin a session with the destination server;

(b) redirecting network communications, including the steps of:

redirecting the handshaking packets by rewriting the destination address in the handshaking packets' IP headers to route the packets to an access controlling web server;

receiving a content request packet from the client machine destined for the destination server intended to retrieve the desired resource from the destination server; and

redirecting the content request packet by rewriting the destination address in the packet IP header to route the packet to the access controlling web server;

(c) receiving a response from the access controlling web server; and

(d) controlling access of the client machine to the desired resource based on the response from the access controlling web server.

18. The computer-readable medium of claim 17, wherein the step of controlling access to the desired resource based on the response from the access controlling web server further comprises the step of:

establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.

19. The computer-readable medium of claim 18, wherein the content request packet comprises a GET URL packet.

20. The computer-readable medium of claim 19, wherein the response indicates that access to the desired resource is allowable if the access controlling web server does not recognize the URL of the GET URL packet.

21. The computer-readable medium of claim 20, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response is that the access controlling web server recognizes the URL of the GET URL packet.

22. The computer-readable medium of claim 19, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

23. The computer-readable medium of claim 22, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

24. The computer-readable medium of claim 22, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

25. The computer-readable medium of claim 24, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

26. The computer-readable medium of claim 19, wherein the response indicates that access to the desired resource is allowable if the access controlling web server recognizes the URL of the GET URL packet.

27. The computer-readable medium of claim 26, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response indicates that the access controlling web server does not recognize the URL of the GET URL packet.

28. The computer-readable medium of claim 27, wherein the access controlling web server is an RSACi Web Server.

29. The computer-readable medium of claim 27, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

30. The computer-readable medium of claim 29, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

31. The computer-readable medium of claim 29, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

32. The computer-readable medium of claim 31, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

Add A7